

**REMARKS**

The Examiner's comments have been carefully considered.

Claims 1, 5, 12, 18, 19, 24, 29, 31, 36, 42, 43, 48, 50, 61, 65, 67, 68, 71, 74, 76, 88, 92, 94, 95, 98, 101, and 108 have been amended to correct the items noted.

The Specification has been amended as noted to correct minor typographical errors resulting from the translation and other matters, including the incorporation of a priority claim.

Claims 1-109 were examined and initially rejected. Applicants have provided amendments to the specification and claims as noted and additional remarks below. As a consequence, Applicants propose that the pending application is now in condition for allowance and notice to that effect is earnestly solicited. Should outstanding issues remain, Applicants respectfully invite the Examiner to call the undersigned for a conference directed to placing the application in condition for allowance.

No new matter has been added. Support for the amendments is found in the original claims, specification, and drawings. Deposit Account Authorization is provided below.

**1. Priority Claim**

Applicants respectfully note that acknowledgment of the perfection of priority to PCT/RU99/00264 filed July 29, 1999 and Russian Application No. 98120922 filed November 25, 1998 is not found within the present paper (confirmation no. 9876). Applicants request acknowledgment of the Priority claim under 35 USC §§119/120/371 etc. in all subsequent action and a clear indication on the record of the full perfection of priority for the pending application.

## **2. Substitute Specification/Amendments to the Specification**

In accordance with 37 C.F.R. §1.125 and MPEP §608.01(q), numerous typographical, format, and arrangement errors resulting from the translation and conversion into the English language required revision. These corrections have been made in the clean and marked-up copy of the specifications provided herein. No new matter has been added and no fees are required for this amendment.

## **3. Drawings**

Applicants respectfully note that acknowledgment of the acceptability of the formal drawings is not shown within the present paper. Applicants respectfully request a clear written indication of the acceptance of the drawings on the record in any subsequent action in the pending matter.

## **4. References**

Applicants respectfully request receipt acknowledgment that the (or any) references provided in the PCT application (of which this application is the national phase the references for which are transferred by requirement of entering the US National Phase) be recognized in any subsequent Office communication (missing here), and specifically request that said PCT references be noted and listed on the face of any published or issued patent.

Applicants have herein provided the results of a preliminary search and an appropriate Information Disclosure Statement and a number of PTO - 1449 form(s). Applicants request the Examiner formally review of these references in due course, formally acknowledge their submission and entry in the record, and that the entire listing of references be listed on the face of any published

or issued patent.

## **5. Responsive Comments**

Before reviewing the Examiners' specific comments and specifically discussing the Nguyen and Chaum references, Applicants wish to first review the "Editor's Note" provided on page 15-16 of the instant office action.

In the Editor's Note it is requested that Applicants "consider the references as potentially teaching all or part of the claimed invention, as well as the context of the passages as taught by the prior art or disclosed by the examiner." Applicants respectfully propose that this request is an improper and inappropriate request for an admission contrary to the burden placed on the Examiner by MPEP §706.02 and §707 (37 C.F.R. 1.104).

The Nguyen and Chaum reference are neither complete in their disclosure nor pioneering in nature. Each reference deals with a similar class 380, but different sub-classes 24 and 3 are officially asserted, supporting their different scopes. In making the present rejection, the Examiner asserts that the references are the "best available art" and, while the Nguyen reference is indeed lengthy, length is not synonymous with disclosure, applicability, or viability as a reference, alone or in combination, the novel items within the claimed invention (discussed below).

It is noted, that the Nguyen reference is merely one of many references in a common area and, as discussed, is lacking in several features alone or in combination with Chaum. The secure electronic payment field includes multiple features allowing many patents (see enclosed IDS/PTO-1449(6-sheets)) focused on separate facets of novelty. If Nguyen were such a blocking reference no further applications would be issued in this subject matter. Applicants urge the Examiner to retain an open mind, despite the breadth and the mind-numbing length and complexity of the Nguyen

reference and indeed the complex nature of other references in this field (enclosed)

**5a. Initial Discussion** (footnotes are used to minimize distraction for long strings)

It is clear that a brief discussion of the Nguyen and Chum references, and the instant application, is necessary to clarify several points.

The patent office has rejected all claims (1-109) of Patent Application Number 09/445,386: “Payment Method and Apparatus Therefor,” on the grounds that these claims are unpatentable over US Patent 6072870 (Nguyen), and in further view of US Patent 4987593 (Chaum). More specifically, it is asserted that Nguyen “discloses the claimed invention” in the independent claims 1, 24, 48, 74, and 101 “except for the payment certificate signature is obtained by means of making a blind money signature of an operator” (Examiner admission)

This initial discussion will explain why the claimed invention is patentable over Nguyen and Chaum. It will show that it is not obvious how to combine the principles of Chaum and Nguyen, and even if it could somehow be done, the result would not be the claimed invention.

**5a(1) Editor and Peer Reviewers Conclude That the Invention Is Novel**

As a first side note, some key elements of the invention were disclosed at the Fifth International Conference on Electronic Commerce after the filing date. This prestigious international conference employed rigorous peer review before selecting a paper on the claimed invention for

publication in its proceedings<sup>1</sup>. This acceptance by those most skilled in the art clearly demonstrates that reviewers found the features of the claimed invention to be novel and significant. A copy of the published paper is attached in the Information Disclosure Statement.

**5a(2) The Claimed Invention Achieves Results That Nguyen Cannot And Includes Features that Nguyen Lacks**

Nguyen teaches that payment information can be received at a gateway, reformatted into a form understood by a host payment application, and then forwarded to that host payment application. Nguyen clearly points out that banks have not converged to a single standard, and many terminals run proprietary protocols (Col. 3, lines 57-65), so there may be value in having a gateway that can perform this reformatting function. Nguyen also clearly states that there are protocols that cannot be mapped or translated universally (Col. 4, lines 14-17).

The core system claimed by Nguyen is built largely on trust, despite the use of certificates and various managers (generally, cols. 87-89). If the operator of the/a gateway or multiple gateways (over multiple internet sites) is dishonest, and the gateway(s) changes or edits the payment information, the Nguyen invention provides no way for either the server or the host payment application to detect, expose, and prove the dishonesty (emphasis added).

For example, where an operator of a server (gateway et al.) is dishonest, and falsely claims that the gateway and the payment application (system including a certificate system) conspired to alter the payment information, the Nguyen invention provides no way for the gateway and/or host payment application to prove their innocence. As disclosed and discussed in Nguyen or Chaum

---

<sup>1</sup> J. M. Peha and I. M. Khamitov, "Pay Cash: A Secure Efficient Internet Payment System," *Proceedings of the Fifth International Conference on Electronic Commerce*, October 2003

(alone or when somehow combined), there is no apparent way that a blind money signature would address these deficiencies. In contrast, the invention claimed in this application does not have these deficiencies. In the claimed invention, if any party or parties in a transaction are dishonest, the honest parties will have irrefutable evidence of their proper conduct that cannot be manipulated.

Another difference between Nguyen and the claimed invention is the degree of anonymity granted the users. For example, with some embodiments of the claimed invention, it is possible to send funds without revealing the identity of the payer to the payee or to the operator of the payment system. Nguyen provides no method to support this level of anonymity. Indeed, it would only be possible to maintain payer anonymity with respect to the gateway in Nguyen if none of the protocols supported by the gateway required the identity of the payer, which would be unusual.

It is not apparent how to add a blind money signature to Nguyen, including the limited blind signature technology taught by Chaum, without making substantial changes to the way Nguyen operates (an impermissible modification unsupported in either reference).

Blind money signatures are used to confer the value associated with this signature to a piece of data, so that the data can be used as a form of “electronic cash.” In the language of this patent application, this produces a *verifiable payment certificate*. Nguyen gives no indication that payment certificates or anything similar will be used and discusses the purpose of “certificates” only to the purpose of “verifying a legitimate cardholder is of [a] valid, branded bankcard number” (col. 86 lines 45-47).

Since the purpose of a blind money signature is to create a valid payment certificate, it is not obvious how a blind money signature (from Chaum) might be used within the scope of the invention

claimed by Nguyen. Any attempts to add payment certificates and blind signatures would be well beyond the scope of issues addressed by Nguyen.

As earlier noted, the Examiner refers to passages where Nguyen does discuss use of a “certificate.” Nguyen teaches that this “certificate” indicates that the certificate authority has checked the payer’s information, and verified that the payer can use a particular payment method (Col. 92, lines 14-63). A merchant can use these certificates during payment to determine whether a consumer has “a valid credit card and good credit,” for example (Col. 93, lines 5-40). This “certificate” as described by Nguyen carries no inherent value, in contrast to the applicant’s “payment certificate” as disclosed and described in the claimed invention, which has received a money signature from the operator. Thus, these “certificate” portions of the Nguyen patent are not particularly relevant to the claimed invention and can be easily distinguished.

MPEP §2143.03 requires that to initially establish a prima facie obviousness rejection of a claimed invention, all the claim limitations must be taught by the prior art, and that all words in a claim must be considered when judging the patentability of an application.

In sum, at least one of the following items is missing from the references (alone or combined) and are claimed in the present invention.

1. Were any party in a transaction is dishonest, the honest parties have irrefutable evidence of their action and honest submission.
2. It is possible for a payer to send funds without revealing their identity to the payee **OR** to the operator of the payment system.
3. Substantial and multiple differences between the instant claimed “certificate” and “blind money” signatures and those previously known. (See comments below clearly distinguishing the prior art from the elements claimed and enabled.)
4. The integrated use of blind money certificates that produces, upon successful use, a verifiable *payment* certificate proving payment without manipulation.

5. The degree of anonymity resulting from the instant invention, which in certain embodiments prohibits knowledge transfer between all players to the transaction.
6. The payer device further comprises a means for creating a payment certificate base by processing a public key and this public key corresponds to the secret key used in the apparatus' "means for forming a payer order signed with a secret key."
7. Finally, another important novel feature of the claimed invention is based on the concept of the "level of a payment certificate" (page 5, lines 14-27), through which it is possible to associate a range of payment values with a single payment certificate. This concept is not supported by either reference.

As a side note, applicants are their own lexicographers (MPEP §2173.01), and it is clear that the claimed use of the word 'certificate' has a different meaning, and hence different limitation and substantial difference from the Nguyen reference. This different meaning for 'certificate' (an actual useful evidentiary payment certificate) has been well disclosed, supported, and claimed in the instant application.

Comparing the similar words and ignore their different requirements is clearly improper and interpreting claim language according to a meaning not dictated by the disclosure would prevent the application of a *prima facie* rejection for obviousness alone. Consequently, it is respectfully suggested that the standard necessary to sustain the preliminary rejection has not been met.

Since each of the independent claims includes at least one limitation or item not found within the applied references each independent claim is *prima facie* nonobvious for that reason alone. Dependent claims depending from allowable independent claims are nonobvious and allowable for that reason alone as well as for the additional recitations they contain.

**5b. Initial Claim review / C 1, 24, 48, 74, and 101 are Novel**

The patent examiner points to passages where Nguyen teaches methods for the generation and processing of payment capture requests and payment capture responses (e.g. Col. 21, lines 17-67, Col. 23, lines 17-61, Col. 20, lines 18-67, and Col. 22, lines 10-25). Unfortunately, these processes differ from the claimed invention in many important respects

As discussed above, one difference is that in the claimed invention, there is a payment certificate which derives value from a blind money signature. The patent examiner correctly points out that the very broad ideas of a payment certificate and blind money signature are known in the art since the time of paper banking; however, the claimed invention is distinct from all prior art in at least the following ways.

One important novel aspect of the claimed invention, which underlies and is required in each independent Claims 1, 24, 48, 74, and 101, is that the payment certificate and the payer order are integrated (page 3, lines 35-39).

More specifically, Claims 1, 24, 48, and 74 all disclose that “a payment certificate base is created in the payer device”<sup>1</sup>, and this payment certificate base includes “an identifier of a public key”<sup>2</sup> which corresponds to “an arbitrary secret key”<sup>3</sup>. Each of these limitations is missing from the references alone or when combined.

---

<sup>1</sup> Claim 1, page 32, lines 2-3. Claim 24, page 35, lines 2-3. Claim 48, page 38, lines 2-3. Claim 74, page 41, lines 2-3.

<sup>2</sup> Claim 1, page 32, line 15. Claim 24, page 35, line 14. Claim 48, page 38, lines 11-12. Claim 74, page 41, lines 11-12.

<sup>3</sup> Claim 1, page 32, line 16. Claim 24, page 35, line 16. Claim 48, page 38, lines 12-13. Claim 74, page 41, lines 12-13.

The “payer order [is] signed with the secret key”<sup>1</sup>. Thus, as required the payment certificate is connected to the payer order through this public-secret key pair in such a way that any attempts to fraudulently alter the order or the payment information can be detected. Consequently, trustworthy records of all transactions are generated.

For example, if the operator falsely claims that a payment certificate is invalid because “the payment certificate was utilized”<sup>2</sup>, there will be evidence to refute this false claim because both the connection and the key pair is lacking or inaccurate. This is not true of other prominent systems known in the art (background section of the application) and indeed is not true of the references Nguyen/Chaum.

Claim 101 similarly connects applicant’s payment certificate to payer order as shown by the following quote. “The payer device further comprises a means for creating a payment certificate base by processing a public key”<sup>3</sup> and this public key corresponds to the secret key used in the apparatus’ “means for forming a payer order signed with a secret key”<sup>4</sup>.

Connecting order and payment certificates in this way is a novel and important feature of the claimed invention, which was not previously disclosed by Nguyen, Chaum, or anyone else. For further discussion on this feature, see Section 5.1 of the attached paper from the Fifth International Conference on Electronic Commerce<sup>5</sup>.

---

<sup>1</sup> Claim 1, page 32, line 18. Claim 24, page 35, line 20. Claim 48, page 38, line 20. Claim 74, page 41, lines 23.

<sup>2</sup> Claim 1, page 32, lines 11-12.

<sup>3</sup> Claim 101, page 44, lines 5-6.

<sup>4</sup> Claim 101, page 44, line 8.

<sup>5</sup> J. M. Peha and I. M. Khamitov, “Pay Cash: A Secure Efficient Internet Payment System,” *Proceedings of the Fifth International Conference on Electronic Commerce*, October 2003

Another important novel feature of the claimed invention is based on the concept of the “level of a payment certificate”<sup>1</sup> (page 5, lines 14-27), through which it is possible to associate a range of payment values with a single payment certificate. This limitation is also lacking from either reference.

For example, in Claims 48 and 74, “the operation of crediting the payment account is carried out in accordance with the excess of the level of the delivered signature above the level of the payment account”<sup>2</sup>. Similarly, in Claim 101, “the blind money signature of the operator is realized using a means for increasing the level of the payment certificate signature”<sup>3</sup>.

It is a novel feature to associate a level with a payment certificate in this way which makes it possible to overcome a number of deficiencies with systems known in the art (Nguyen/Chaum), such as the need to store information on every certificate that has been used (page 2, line 41 to page 3, line 3). Neither Nguyen nor Chaum use this approach. For further discussion on this feature, see Section 5.2 of the attached paper from the Fifth International Conference on Electronic Commerce<sup>4</sup>.

### **5c. The Claimed Invention Is Not Disclosed by Chaum**

Patent 4,987,593 (Chaum) on “One-show Blind Signature Systems” is related, but does not disclose, and cannot cover, any of the core ideas of the claimed invention.

The patent examiner says that “Chaum teaches that it is known in the art to provide a

---

<sup>1</sup> Page 5, line 14.

<sup>2</sup> Claim 48, page 38, lines 18-20. Claim 74, page 41, lines 21-23.

<sup>3</sup> Claim 101, page 44, lines 15-17.

<sup>4</sup> J. M. Peha and I. M. Khamitov, “Pay Cash: A Secure Efficient Internet Payment System,” *Proceedings of the Fifth International Conference on Electronic Commerce*, October 2003

payment certificate signature that is obtained by means of making a blind money signature of an operator.” In contradiction, the idea of a blind money signature was known and discussed in the open literature long before Chaum’s Patent, as this patent application discloses (page 2, line 19 to page 3, line 3).

As used in Chaum, a blind money signature requires a digital signature from the operator. If a blind digital signature is desired, there are a number of systems known in the art that will suffice, some of which are referenced in the patent application (page 6, lines 31-35). The claimed invention can work with any of these after modifying their structure to suit the needs of the claimed invention. A description of any particular blind signature system, including Chaum, does not disclose the novel features of the claimed invention.

Moreover, in the claimed invention, applicants “blind money signature” (defined for this invention on page 6) does not require use of a blind digital signature. The claimed invention gives “the possibility of obtaining blind digital signature” (page 6, line 30). In one embodiment of the invention where the “blind money signature” is a digital signature that is not blind, the operator will gain the ability to trace payments in some cases, but the invention will otherwise work and meet all its other objectives stated therein.

#### **5d. Other Claims**

For the reasons above, independent Claims 1, 24, 48, 74, and 101 are patentable over both Nguyen and Chaum as including at least one additional element or limitation not shown or taught in the reference applied. Consequently, each dependant claim, being dependent upon an allowable base claim is similarly allowable. In sum, applicants propose that claims 1-109 are patentable over both Nguyen and Chaum.

**5e. The Role of Unblinding: Claims 3, 25, 52, 78, and 104**

To clarify it may help if I say more about “unblinding” as used herein. In response to Claims 3, 25, 52, 78, and 104, the Examiner states that “it would have been obvious to one having ordinary skill in the art at the time of the invention was made that the term “unblinding” refers to decrypting the data for viewing since it is known in the art that when you decrypt data, you expose or unblind the data for processing.” Unfortunately, this assertion is false and lacks any actual basis other than as a loose descriptive.

Actually, it is known in the art that “unblinding” is not synonymous with “decrypting” (see J. Phea article “Pay Cash: A Secure Internet Payment System” and other previously identified references)

It is often the case that when you ‘decrypt’ data, you do not ‘unblind’ anything. As an example, if  $B(.)$  and  $B^{-1}(.)$  are blinding and unblinding functions, respectively, they have the following property:

$$B^{-1}(f(B(X))) = f(X)$$

for some function  $f(.)$  and any number  $X$ .

Decryption functions do not necessarily have this property (they merely decrypt, they do not necessarily unblind). In addition, it is typically difficult to determine  $X$  from  $B(X)$  for those who do not know the specific underlying unblinding function  $B^{-1}(.)$ .

A blinding function is useful because an operator can apply a function  $f$  (such as a money signature) to  $X$  without ever knowing  $X$ .  $X$  is blinded with  $B(\cdot)$ , then the operator applies function  $f(\cdot)$  to  $B(X)$  without seeing  $X$ , and then  $f(B(X))$  is unblinded to produce  $f(X)$ .

There is no obvious way to add unblinding to the ideas disclosed in the passages by Nguyen identified by the patent examiner (Col. 87-88, lines 1-67) and consequently this assertion lacks any support other than improper speculation.

## CONCLUSION

Applicants have respectfully shown that a *prima facie* rejection has not been made, and for the reasons noted above, cannot be made. Applicants propose that the independent claims each include at least one additional feature, limitation, or function not fairly found in the applied art and that the claims are allowable for that reason alone.

Where an unsupported assertion of obviousness is made applicants have rebutted and should the objections are maintained despite Applicants' amendments and herein seasonable traversal of the *prima facie* rejection and request for supportive written documents capable of review and rebuttal by experts on appeal, Applicants specifically request under MPEP §2144.03 (c) and §2163.04, that the Examiner provide both written evidence, in an affidavit 'offer of proof,' that establishing the ordinary skill in the art based on the Examiner's own personal knowledge, and that those ordinary skill in the art would find each and every one of the necessary redesign modifications noted above as obvious to one skilled in the art absent impermissible hindsight reasoning.

As an aside, Applicants note that it is the prior art itself that "must provide the motivation or reason for the worker in the art, without the benefit of [applicants] specification, to make the

necessary changes in the reference device.” MPEP 2144.04 (C). The other requirements for reaching a *prima facie* obviousness rejection are well known and incorporated here.

Applicants respectfully submit that the combination of references, proposed by the Examiner, neither teach or suggest, all of the claim limitations of the present invention, nor provide a suggested desirability for the necessary modifications and additions, nor provide a reasonable expectation of success without further modification. Reconsideration and withdrawal of all rejections is respectfully requested. In view of the foregoing (including claim amendments), the application is now believed to be in proper form for allowance and notice to that effect is earnestly solicited.

While Applicants have respectfully disagreed with the rejection of the claims for the above reasons, Applicants have elected to amend the claims to eliminate typographical errors or language issues transferring from the foreign translation for the purpose of clarifying for the public the patent application in a manner consistent with the PTO’s Patent Business Goals (PBG), 35 Fed. Reg. 54603 (September 8, 2000). Therefore, it is proposed that these amendments (claim and specification) do not narrow the scope of interpretation for the claims.

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or to credit any overpayment related hereto, to Deposit Account No. 010-0100. No new matter has been added.

While Applicants believe that they have overcome the Examiner’s initial *prima facie* obviousness rejections, if the Examiner believes that a telephone conference would be of value to place the application in condition for allowance, the Examiner is respectfully requested to call the undersigned counsel at the number listed below for resolution of any remaining issues placing the application in condition for allowance. An early and favorable action is respectfully solicited.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read 'A. Young', with a stylized flourish at the end.

Andrew Young, Esq.  
Registration No. 44,001  
Attorney for Applicant

**Lackebach Siegel, LLP**  
Lackebach Siegel Building  
One Chase Road  
Scarsdale, NY 10583  
Phone: 914-723-4300  
Facsimile: 914-723-7301  
Date: April 5, 2004

P-9902.aml responsive amendment.wd.wpd

Note:

A "Clean Copy" of the claims is no longer required and is not attached

Attached is a clean and marked-up version of the substitute specification under §1.125